UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,220	12/09/2005	Yun Kyung Lee	CU-4590 WWP	2686

26530   7590   12/24/2008

LADAS & PARRY LLP
224 SOUTH MICHIGAN AVENUE
SUITE 1600
CHICAGO, IL 60604

EXAMINER
SIMS, JING F

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
12/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☒ Claim(s) *1, 3, 5, 9, and 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to communications: application 10/560,020 filed on

December 9th, 2005; amendment filed on October 23rd, 2008.

2.   Claims 1, 3, 5, 9, and 11 are amended.

3.   Applicant's arguments, with respect to claims 1-12, have been fully considered

but they are not persuasive.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

5.   Claims 1, 3, 5, 9 and 11 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject matter

which the Applicant regards as the invention.

Claims 1, 3, 5, 9 and 11 recites the limitation "a first M/m input data" and "a

second M/m input data" in the last 2 lines of the claim. There is insufficient antecedent

basis for this limitation in the claim. For example, if "a first M/m input data" means to be

the lower 64-bit data, and "a second M/m input data" means to be the upper 64-bit

data", then the round keys generated in the add-round-key generation unit is added to

the lower 64-bit data, which does not simultaneously process the upper 64-bit data.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

9.   **Claims 1-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Yang (US 2002/0131588), in view of Lee et al. (US Application Publication US

2005/0135607 A1) (hereinafter Lee).

As per claim 1, Yang discloses "A rijndael block encryption apparatus having M-

bit input data and N-bit input keys" (page 1, column 2, paragraph 0010, "an apparatus

for encrypting/decrypting a real-time input stream". With respect to the limitations of

input data and input keys, in Fig. 1 Data_in [7:0] appears to be the input data and

Key_data [128,192,256] appear to be the inputs keys) "and encrypting the M-bit input

data by repeating for a predetermined number of times a round operation" (page 3,

column 1, paragraph 0043, with respect to this limitation, Yang discloses "if the block

size is 128 bits and a size of the key value is 256 bits, a count of rounds becomes '14'"

"if the block size is 128 bits and a size of the key value is 128 bits, a count of rounds

becomes '10'") "that includes transforms of shift_row, substitution, mixcolumn and add-

round-key" (Fig. 4 discloses "Shifter (Shift_row)", "Data conversion unit (Byte_sub)",

"Mixer (Mix_colm)", and "Key mixer (Add_round_key)) "the apparatus comprising: a

round operation unit including a round operation execution unit for processing the data

at least in the transforms of substitution, mixcolumn and add-round-key" (page 3,

column 2, paragraph 0048, "Fig. 4 illustrates a detailed block diagram of an encryption

unit of 'the block round unit' 203 in Fig. 2". Fig. 4 illustrates the transforms of "Shifter

(Shift_row)", "Data conversion unit (Byte_sub)", "Mixer (Mix_colm)", and "Key mixer

(Add_round_key)) "and a round key generation unit for generating round keys in order

to provide the round keys in the transform of the add-round-key; a round operation

control unit for controlling the round operation performed by the round operation unit"

(page 1, paragraph 0013, "a key schedule unit carrying out a key schedule every round

in accordance with a size and a key value of a block inputted from outside so as to

output a key value for the encryption or decryption each round") "and a data storage unit

for storing M-bit data generated at an end stage of every round." (Page 4, column 1,

paragraph 0057, "an output buffer 603 receiving the encrypted or decrypted data

Out_block [127:0]").

However, Yang fails to disclose "processing the data in the unit of M/m bits

(where m is 2, 3 or 4)", and "a data storage unit for storing M/m-bit intermediate data

generated by the round operation unit at an intermediate stage of every round, wherein

the round keys generated in the add-round-key generation unit is added to a first M/m

input data simultaneously during the processing of a second M/m input data of the

round execution unit before the end stage of every round".

Lee discloses "processing the data in the unit of M/m bits (where m is 2, 3 or 4)"

(page 2, [0022], simultaneously executing data input and data processing through

parallel-processing AES rounds using a plurality of input data handling routines; [0023],

receiving a plurality of divided part of an input data) and "storing M/m-bit intermediate

data generated by the round operation unit at an intermediate stage of every round"

(Fig. 4 and page 4, [0054], the first to fourth registers 104 to 404 are input with the

output data from the first round key adder 339; Fig. 3, page 3, [0048], the register stores

the data for a predetermined time, performs shift operation, and input data to the first

selector, thus executing second round operations), "wherein the round keys generated

in the add-round-key generation unit is added to a first M/m input data simultaneously

during the processing of a second M/m input data of the round execution unit before the

end stage of every round" (page 4, [0064], the encryption and decryption apparatus has

two separate operation routines, and each operation routine are independently

operated. Accordingly, the operations of each round are performed in parallel following

the two separate routines. Table 1, round 2, cycle 4, the Second round key adder adds

the round key RKey B to the second divided part of the input data simultaneously during

the First byte substitution part and/or First column mixer process the first divided part of

the input data before the end stage of every regular round).

Yang and Lee are analogous art because they are from the same field of

endeavor of performing Rijndael block cipher for encryption and decryption.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of invention to modify the teaching of Yang to use Rijndael cipher encrypting and

decrypting input data by performing the operations of each round in parallel that taught

by Lee because it would provide rapidly perform an encryption and decryption (see Lee

page 1, [0003]).

As per claim 2, Yang discloses "the apparatus as claimed in claim 1, wherein the data storage unit includes at least one register, and a total summed size of the register is equal to or larger than M (2m-1)/m bits" (Fig. 5 and Fig. 6, registers are intermediate storage units, therefore, the Examiner considers unit 500 in Fig. 5 is a storage unit, unit 603 in Fig. 6 is the other storage unit. There are two set of storage units, which includes four individual registers in unit 500 in Fig. 5 of total 508 bits - 127 bit multiplies 4, plus the "out_buffer" storage in Fig. 6 of 127 bit. The total summed sized of the register is 635 bit. As applicant states in claim 1 "where m is 2, 3, or 4", if m is 2, M the input data in Yang is 127 bit, then M(2m-1)/m is 127(2*2-1)/2 that equals 190.5 bits. The total summed sized of the registers in Yang of 635 bit is large than the 190.5 bit).

As per claim 3, Yang discloses "A rijndael block decryption apparatus having M-bit input data and N-bit input keys" (page 1, column 2, paragraph 0010, "an apparatus for encrypting/decrypting a real-time input stream" "by constructing Rijndael algorithm selected as AES algorithm with hardware". With respect to the limitations of input data and input keys, in Fig. 1 Data_in [7:0] appears to be the input data and Key_data [128,192,256] appear to be the inputs keys) "and decrypting the M-bit input data by repeating for a predetermined number of times a round operation" (page 3, column 1, paragraph 0043, with respect to this limitation, Yang discloses "decrypting" by "finding the key for encryption or decryption". Yang also discloses "if the block size is 128bits and a size of the key value is 256 bits, a count of rounds becomes '14'" "if the block size is 128 bits and a size of the key value is 128 bits, a count of rounds becomes '10'") "that includes transforms of inverse shift_row, inverse substitution, add-round-key and

inverse mixcolumn" (Fig. 5 discloses transforms of "I_shift_row", "I_byte_sub",

"Add_round_key", and "I_mix_colm") "the apparatus comprising: a round operation unit

including a round operation execution unit for processing the data at least in the

transforms of inverse substitution, add-round-key and inverse mixcolumn" (page 3,

column 2, paragraph 0048, "Fig. 4 illustrates a detailed block diagram of an encryption

unit of 'the block round unit' 203 in Fig. 2". Fig. 4 illustrates the transforms of "Shifter

(Shift_row)", "Data conversion unit (Byte_sub)", "Mixer (Mix_colm)", and "Key mixer

(Add_round_key)). Yang also discloses "if the decryption is being carried out, the

encryption in Fig. 4 is carried out in reverse. The reverse process is shown in Fig. 5")

"and a round key generation unit for generating round keys in order to provide the round

keys in the transform of add-round-key; a round operation control unit for controlling the

round operation performed by the round operation unit" (page 1, paragraph 0013, "a key

schedule unit carrying out a key schedule every round in accordance with a size and a

key value of a block inputted from outside so as to output a key value for the encryption

or decryption each round") "and a data storage unit for storing M-bit data generated at

an end stage of every round" (the rejection of the corresponding section in claim 1 also

applies here in claim 2).

However, Yang fails to disclose "processing the data in the unit of M/m bits

(where m is 2, 3 or 4)", and "a data storage unit for storing M/m-bit intermediate data

generated by the round operation unit at an intermediate stage of every round, wherein

the round keys generated in the add-round-key generation unit is added to a first M/m

input data simultaneously during the processing of a second M/m input data of the

round execution unit before the end stage of every round".

Lee discloses "processing the data in the unit of M/m bits (where m is 2, 3 or 4)"

(page 2, [0022], simultaneously executing data input and data processing through

parallel-processing AES rounds using a plurality of input data handling routines; [0023],

receiving a plurality of divided part of an input data) and "storing M/m-bit intermediate

data generated by the round operation unit at an intermediate stage of every round"

(Fig. 4 and page 4, [0054], the first to fourth registers 104 to 404 are input with the

output data from the first round key adder 339; Fig. 3, page 3, [0048], the register stores

the data for a predetermined time, performs shift operation, and input data to the first

selector, thus executing second round operations), "wherein the round keys generated

in the add-round-key generation unit is added to a first M/m input data simultaneously

during the processing of a second M/m input data of the round execution unit before the

end stage of every round" (page 4, [0064], the encryption and decryption apparatus has

two separate operation routines, and each operation routine are independently

operated. Accordingly, the operations of each round are performed in parallel following

the two separate routines. Table 1, round 2, cycle 4, the Second round key adder adds

the round key RKey B to the second divided part of the input data simultaneously during

the First byte substitution part and/or First column mixer process the first divided part of

the input data before the end stage of every regular round).

Yang and Lee are analogous art because they are from the same field of

endeavor of performing Rijndael block cipher for encryption and decryption.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Yang to use Rijndael cipher encrypting and decrypting input data by performing the operations of each round in parallel that taught by Lee because it would provide rapidly perform an encryption and decryption (see Lee page 1, [0003]).

As per claim 4, Yang discloses "the apparatus as claimed in claim 3, wherein the data storage unit includes at least one register, and a total summed size of the register is equal to or larger than M (2m-1)/m bits" (Fig. 5 and Fig. 6, registers are intermediate storage units, therefore, there are four registers in Fig. 5 of total 508 bits - 127 bit multiplies 4, plus the "out_buffer" storage in Fig. 6 of 127 bit. The total summed sized of the register is 635 bit. As applicant states in claim 1 "where m is 2, 3, or 4", if m is 2, M the input data in Yang is 127 bit, then M(2m-1)/m is 127(2*2-1)/2 that equals 190.5 bits. The total summed sized of the registers in Yang of 635 bit is large than the 190.5 bit).

As per claim 5, Yang discloses "A rijndael block encryption apparatus having M-bit input data and N-bit input keys" (page 1, column 2, paragraph 0010, "an apparatus for encrypting/decrypting a real-time input stream" "by constructing Rijndael algorithm selected as AES algorithm with hardware". With respect to the limitations of input data and input keys, in Fig. 1 Data_in [7:0] appears to be the input data and Key_data [128,192,256] appear to be the inputs keys) "and encrypting the M-bit input data by repeating for a predetermined number of times a round operation for encryption" (page 3, column 1, paragraph 0043, with respect to this limitation, Yang discloses "if the block size is 128 bits and a size of the key value is 256 bits, a count of rounds becomes '14'"

"if the block size is 128 bits and a size of the key value is 128 bits, a count of rounds

becomes '10'") "that includes transforms of shift_row, substitution, mixcolumn and add-

round-key" (Fig. 4 discloses "Shifter (Shift_row)", "Data conversion unit (Byte_sub)",

"Mixer (Mix_colm)", and "Key mixer (Add_round_key)) "or decrypting the M-bit input

data by repeating for a predetermined number of times a round operation" (page 3,

column 1, paragraph 0043, with respect to this limitation, Yang discloses "decrypting" by

"finding the key for encryption or decryption". Yang also discloses "if the block size is

128 bits and a size of the key value is 256 bits, a count of rounds becomes '14'" "if the

block size is 128 bits and a size of the key value is 128 bits, a count of rounds becomes

'10'") "for decryption that includes transforms of inverse shift_row, inverse substitution,

add-round-key and inverse mixcolumn" (page 3, column 1, paragraph 0043, with

respect to this limitation, Yang discloses "decrypting" by "finding the key for encryption

or decryption". Yang also discloses "if the block size is 128bits and a size of the key

value is 256 bits, a count of rounds becomes '14'" "if the block size is 128 bits and a

size of the key value is 128 bits, a count of rounds becomes '10'") "the apparatus

comprising: a round operation unit including a round operation execution unit for

processing the data at least in the transforms of substitution, mixcolumn and add-round-

key in an encryption mode" (Fig. 4, the block round unit serves the same function as

round operation unit. It includes at least substitution which in instant application "data

conversion unit(byte_sub)", mixcolumn which in instant application "mixer", and add-

round-key which in instant application "key mixer") "and for processing the data at least

in the transforms of inverse substitution, add-round-key and inverse mixcolumn in a

decryption mode" (Fig. 5, the block round unit includes at least inverse substitution

which in instant application "data conversion unit(I_byte_sub)", add-round-key which in

instant application "key mixer", and mixcolumn which in instant application "inverse

mixer") "and a round key generation unit for generating round keys in order to provide

the round keys in the transform of add-round-key; a round operation control unit for

controlling the round operation performed by the round operation unit" (page 1,

paragraph 0013, "a key schedule unit carrying out a key schedule every round in

accordance with a size and a key value of a block inputted from outside so as to output

a key value for the encryption or decryption each round"); "and a data storage unit for

storing M-bit data generated at an end stage of every round" (page 4, column 1,

paragraph 0057, "an output buffer 603 receiving the encrypted or decrypted data

Out_block[127:0]").

However, Yang fails to disclose "processing the data in the unit of M/m bits

(where m is 2, 3 or 4)", and "a data storage unit for storing M/m-bit intermediate data

generated by the round operation unit at an intermediate stage of every round, wherein

the round keys generated in the add-round-key generation unit is added to a first M/m

input data simultaneously during the processing of a second M/m input data of the

round execution unit before the end stage of every round".

Lee discloses "processing the data in the unit of M/m bits (where m is 2, 3 or 4)"

(page 2, [0022], simultaneously executing data input and data processing through

parallel-processing AES rounds using a plurality of input data handling routines; [0023],

receiving a plurality of divided part of an input data) and "storing M/m-bit intermediate

data generated by the round operation unit at an intermediate stage of every round"

(Fig. 4 and page 4, [0054], the first to fourth registers 104 to 404 are input with the

output data from the first round key adder 339; Fig. 3, page 3, [0048], the register stores

the data for a predetermined time, performs shift operation, and input data to the first

selector, thus executing second round operations), "wherein the round keys generated

in the add-round-key generation unit is added to a first M/m input data simultaneously

during the processing of a second M/m input data of the round execution unit before the

end stage of every round" (page 4, [0064], the encryption and decryption apparatus has

two separate operation routines, and each operation routine are independently

operated. Accordingly, the operations of each round are performed in parallel following

the two separate routines. Table 1, round 2, cycle 4, the Second round key adder adds

the round key RKey B to the second divided part of the input data simultaneously during

the First byte substitution part and/or First column mixer process the first divided part of

the input data before the end stage of every regular round).

Yang and Lee are analogous art because they are from the same field of

endeavor of performing Rijndael block cipher for encryption and decryption.

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of invention to modify the teaching of Yang to use Rijndael cipher encrypting and

decrypting input data by performing the operations of each round in parallel that taught

by Lee because it would provide rapidly perform an encryption and decryption (see Lee

page 1, [0003]).

As per claim 6, Yang discloses "the apparatus as claimed in claim 5, wherein the

round operation execution unit comprises:" (page 3, paragraph 0048, paragraph 0053,

"Fig. 4 illustrates a detailed block diagram of an encryption unit of the block round unit

203 in Fig. 2 and Fig. 5 illustrates a detailed block diagram of a decryption unit 500 of

the block round unit in Fig. 2" and "if the decryption is being carried out, the encryption

in Fig. 4 is carried out is in reverse") "a shift/inverse-shift_row operation means for

performing the shift_row operation and the inverse shift_row operation of the data;" (Fig.

4, Fig. 5, "shifter(shift_row)" in Fig. 4 and "Inverse shift(I_shift_row)" in Fig. 5) "a

substitution/inverse-substitution operation means for performing the substitution

operation and the inverse substitution operation of the data" (Fig. 4, Fig. 5, "Data

conversion unit (byte_sub)" in Fig. 4 and "data conversion unit (I_byte_sub)" in Fig. 5) "a

mixcolumn/inverse-mixcolumn operation means for performing the mixcolumn operation

and the inverse mixcolumn operation of the data" (Fig. 4, Fig. 5, "Mixer(Mix_colm) in

Fig. 4, and "Inverse mixer(I_mix_colm)" in Fig. 5) "and an add-round-key operation

means for performing the add-round-key operation of the data" (Fig. 4 and Fig. 5, "Key

Mixer(Add_round_key)" in Fig. 4 and "Key mixer (Add_round_key)" in Fig. 5)

As per claim 7, Yang discloses "the apparatus as claimed in claim 6, wherein the

round operation execution unit farther comprises a plurality of demultiplexing means for

controlling a flow of the data among the substitution/inverse-substitution operation

means, the mixcolumn/inverse-mixcolumn operation means and the add-round-key

operation means so as to perform the round operation for the encryption or the round

operation for the decryption according to an input of a mode signal that indicates the

encryption or decryption mode" (Fig. 1 or Fig. 2, paragraph 0036, "signals inputted to

the block round unit 203 include wsel[1:0] informing a size of a key value, Encrypt_en

signal informing whether to be encrypt or decrypt").

As per claim 8, Yang discloses "the apparatus as claimed in any one of claims 5

to 7, wherein the data storage unit includes at least one register, and a total summed

size of the register is equal to or larger than M $(2m-1)/m$ bits" (Fig. 5 and Fig. 6,

registers are intermediate storage units, therefore, there are four registers in Fig. 5 of

total 508 bits - 127 bit multiplies 4, plus the "out_buffer" storage in Fig. 6 of 127 bit. The

total summed sized of the register is 635 bit. As applicant states in claim 1 "where m is

2, 3, or 4", if m is 2, M the input data in Yang is 127 bit, then $M(2m-1)/m$ is 127(2*2-1)/2

that equals 190.5 bits. The total summed sized of the registers in Yang of 635 bit is

large than the 190.5 bit).

10.   **Claims 9-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Yang (US 2002/0131588), in view of Roussel et al. (US patent, US 6,230,257 B1)

(hereinafter Roussel), and further in view of Lee et al. (US Application Publication US

2005/0135607 A1) (hereinafter Lee).

As per claim 9, Yang discloses "a rijndael block encryption method for receiving

M-bit input data and N-bit input keys and performing a round operation of the input data

for a predetermined number of times, the method comprising:" (page 1, column 2,

paragraph 0010, "an apparatus for encrypting/decrypting a real-time input stream" "by

constructing Rijndael algorithm selected as AES algorithm with hardware". With respect

to the limitations of input data and input keys, in Fig. 1 Data_in [7:0] appears to be the

input data and Key_data [128,192,256] appear to be the inputs keys. On page 3,

column 1, paragraph 0043, with respect to predetermined number of times, Yang also

discloses "if the block size is 128bits and a size of the key value is 256 bits, a count of

rounds becomes '14'" "if the block size is 128 bits and a size of the key value is 128 bits,

a count of rounds becomes '10'") "a round operation step of performing a round

operation with respect to all m data of M/n bits" (page 3, column 1, paragraph 0043,

Yang discloses "if the block size is 128bits and a size of the key value is 256 bits, a

count of rounds becomes '14'" "if the block size is 128 bits and a size of the key value is

128 bits, a count of rounds becomes '10'. It shows the relation between the number of

round for performing round operation and the input data size in Rijndael cipher in the

above paragraph; therefore, a round operation stop with respect to input data 'M' bit or

'M/n' bit (if M/n equals to M. The claim indicates m data belong to M/n, then a round

operation stop with respect to all m as well.) "The round operation including sub-steps of

a shift_row transform for performing a shift_row of the M-bit data from a previous round"

(Fig. 2, and Fig. 4, "the block round unit" in Fig. 2 includes a "shifter (Shift_row)" in Fig.

4 to perform a shift_row of 128 bits [127:0] input data from previous round and

outputting data to next transform) "a substitution transform for performing a substitution

data, a mixcolumn transform for performing a mixcolumn of data" (Fig. 4, "Data

conversion unit (Byte_sub)" to perform a substitution data, "Mixer (Mix_colm)" to

perform a mixcolumn data) "and an add-round-key transform for performing an addition

of round" (it is a known for one skilled in the art at the invention time that to repeating

either one specific or plurality additional transform steps when to perform a round

operation in Rijndael block cipher system during the encryption transformation) "and a round key generation step of generating the round keys in order to provide the round keys at the sub-step of the add-round-key transform" (Fig. 2, and page 3, paragraph 0039-0047, "the Key schedule unit"[reference number 202 in Fig. 2] "find a key for encrypting or decrypting each round so as to output the found key to the block round unit 203").

However, Yang fails to disclose "a shift_row transform outputting only M/m-bit (where m is 2, 3 and 4) data corresponding to a selection signal to a next step", "a substitution transform performing of the M/m-bit data and mixcolumn transform performing of the M/m-bit data" and "keys having the same size to the M/m-bit data" and "wherein the round keys generated in the add-round-key generation unit is added to a first M/m input data simultaneously during the processing of a second M/m input data of the round execution unit before the end stage of every round".

Roussel discloses "outputting only M/m-bit (where m is 2, 3 and 4) data corresponding to a selection signal to a next step" (column 7, line 53-63, "execution units 130 and 140 generate output data as two half width data segments". "Two half width data segments" means the width of input data M divided by 2 where m is 2. "Low order data is output at an OUTLO terminal. High order data is output one clock cycle later at an OUTHI terminal. The low and high order output data propagate through separate drivers 330 and 340 to the low and high local bypass buses 310 and 320 respectively" serves the function of "selection signal to a next step"). Roussel also discloses "a substitution transform performing of the M/m-bit data and mixcolumn

transform performing of the M/m-bit data" and "keys having the same size to the M/m-bit data" " (these two limitations limit same thing which is to divide the width of the input data to sub sets to reduce the size hardware. With respect to this limitation, Roussel discloses "processing 128-bit instructions using existing 64-bit hardware systems without significant changes to the hardware" (column 12, line 1-9)).

Lee discloses "wherein the round keys generated in the add-round-key generation unit is added to a first M/m input data simultaneously during the processing of a second M/m input data of the round execution unit before the end stage of every round" (page 4, [0064], the encryption and decryption apparatus has two separate operation routines, and each operation routine are independently operated. Accordingly, the operations of each round are performed in parallel following the two separate routines. Table 1, round 2, cycle 4, the Second round key adder adds the round key RKey B to the second divided part of the input data simultaneously during the First byte substitution part and/or First column mixer process the first divided part of the input data before the end stage of every regular round).

Yang, Roussel, and Lee are analogous art because they are in the same field of utilizing existing hardware to design circuits for an apparatus.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Yang and Lee to use Rijndael block cipher algorithm encrypting/decrypting information that described by Yang, and apply "staggering execution of a single packed data instruction using the same circuit" from Roussel to utilize the existing hardware resource, reduce the size and cost of hardware.

As per claim 10, Yang in view of Roussel disclose claim 9 and "wherein the data

can be processed through the steps of the shift_row transform, the substitution

transform, the mixcolumn transform and the add-round-key transform, respectively" (see

Yang, Fig. 4 discloses Shift (Shift_row), Data conversion unit (Byte_sub), Mixer

(Mix_colm), and Key Mixer (Add_round_key)) "the data having the size of M/m bits"

(see Roussel, column 12, line 1-9, "processing 128-bit instructions using existing 64-bit

hardware systems without significant changes to the hardware) and "a plurality of the

M/m-bit data can be processed through the plural steps selected among the four steps

at the same time according to a predetermined timing" (see Roussel, Fig. 4A and Fig.

4B, Fig. 4A discloses a plurality of the input data "M" with the width of 128 bits is divided

by two of the 64 bits data after ports 1-3. Fig. 4B shows that at same time T, plural

steps, to be exact two steps, have been processed. Four steps have been processed at

time T+1 etc).

As per claim 11, Yang discloses "A rijndael block decryption method for receiving

M-bit input data and N-bit input keys and performing a round operation of the input data

for a predetermined number of times, the method comprising:" (page 1, column 2,

paragraph 0010, "an apparatus for encrypting/decrypting a real-time input stream" "by

constructing Rijndael algorithm selected as AES algorithm with hardware". With respect

to the limitations of input data and input keys, in Fig. 1 Data_in [7:0] appears to be the

input data and Key_data [128,192,256] appear to be the inputs keys. On page 3,

paragraph 0043, with respect to the limitation "predetermined number of times", Yang

discloses "if the block size is 128bits and a size of the key value is 256 bits, a count of

rounds becomes '14'" "if the block size is 128 bits and a size of the key value is 128 bits,

a count of rounds becomes '10'") "A round operation step of performing a round

operation with respect to all m data of M/n bits" (page 3, paragraph 0043, Yang

discloses "if the block size is 128bits and a size of the key value is 256 bits, a count of

rounds becomes '14'" "if the block size is 128 bits and a size of the key value is 128 bits,

a count of rounds becomes '10'. It shows the relation between the number of round for

performing round operation and the input data size in Rijndael cipher in the above

paragraph; therefore, a round operation stop with respect to input data 'M' bit or 'M/n' bit

(if M/n equals to M. The claim indicates m data belong to M/n, then a round operation

stop with respect to all m as well.) "the round operation including sub-steps of an

inverse shift_row transform for performing an inverse shift_row of the M-bit data from a

previous round and outputting data" (Fig. 5, "Inverse shifter (I_shift_row)to perform an

inverse shift row of 128 bits [127:0] data and outputting to next transform) "an inverse

substitution transform for performing an inverse substitution inverse-shift_row-

transformed data" (Fig. 5, Data conversion unit (I_byte_sub) to perform an inverse

substitute on the output data of Inverse shifter (I_shift_row)) "an add-round-key

transform for performing an addition of round keys having the same size to inverse-

substitution-transformed data, respectively, " (Fig. 5, Key mixer (Add_round_key) to

perform a add round key transform. Fig. 5 discloses both Add_round_key and

I_byte_sub have the same size data of 128 bits [127:0]. The decryption transformation

order of I-shift_row, I_byte_sub, and Add_round_key in Fig. 5 respects to the

corresponding encryption order in Fig. 4) "and an inverse mixcolumn transform for

performing an inverse mixcolumn add-round-key-transformed data" (Fig. 5, Inverse

mixer (I_mix_colm) to perform inverse mix column on Add_round_key data) "and a

round key generation step of generating the round keys in order to provide the round

keys at the sub-step of the add-round-key transform". (Fig. 2, and page 3, paragraph

0039-0047, "the Key schedule unit"[reference number 202 in Fig. 2] "find a key for

encrypting or decrypting each round so as to output the found key to the block round

unit 203").

Yang fails to disclose "an inverse shift_row transform outputting only M/m-bit

(where m is 2, 3 and 4) data corresponding to a selection signal to a next step", "for

performing an inverse substitution of the M/m-bit data" "round keys having the same

size to the M/m-bit inverse-substitution-transformed data" and "an inverse mixcolumn of

the M/m-bit add-round-key-transformed data".

However, Roussel discloses "outputting only M/m-bit (where m is 2, 3 and 4) data

corresponding to a selection signal to a next step" (column 7, line 53-63, "execution

units 130 and 140 generate output data as two half width data segments". "Two half

width data segments" means the width of input data M divided by 2 where m is 2. "Low

order data is output at an OUTLO terminal. High order data is output one clock cycle

later at an OUTHI terminal. The low and high order output data propagate through

separate drivers 330 and 340 to the low and high local bypass buses 310 and 320

respectively" serves the function of "selection signal to a next step"). Roussel also

discloses "for performing an inverse substitution of the M/m-bit data" "round keys having

the same size to the M/m-bit inverse-substitution-transformed data" and "an inverse

mixcolumn of the M/m-bit add-round-key-transformed data" (the three limitations limit

same thing which is to divide the width of the input data to sub sets to reduce the size

hardware. With respect to this limitation, Roussel discloses "processing 128-bit

instructions using existing 64-bit hardware systems without significant changes to the

hardware" (see column 12, line 1-9)).

Lee discloses "the round keys generated in the add-round-key generation unit is

added to a first M/m input data simultaneously during the processing of a second M/m

input data of the round execution unit before the end stage of every round" (page 4,

[0064], the encryption and decryption apparatus has two separate operation routines,

and each operation routine are independently operated. Accordingly, the operations of

each round are performed in parallel following the two separate routines. Table 1,

round 2, cycle 4, the Second round key adder adds the round key RKey B to the second

divided part of the input data simultaneously during the First byte substitution part

and/or First column mixer process the first divided part of the input data before the end

stage of every regular round).

Yang, Roussel, and Lee are analogous art because they are in the same field of

utilizing existing hardware to design circuits for an apparatus.

It would have been obvious to one of ordinary skill in the art at the time of

invention to modify the teaching of Yang and Lee to use Rijndael block cipher algorithm

encrypting/decrypting information that described by Yang, and apply "staggering

execution of a single packed data instruction using the same circuit" from Roussel to

utilize the existing hardware resource, reduce the size and cost of hardware.

As per claim 12, Yang in view of Roussel disclose claim 11, and "wherein the data can be processed through the steps of the inverse shift_row transform, the inverse substitution transform, the add-round-key transform and the inverse mixcolumn transform, respectively" (see Yang, Fig. 5 discloses transforms of data through "I_shift_row", "I_byte_sub", "Add_round_key", and "I_mix_colm"); "the data having the size of M/m bits" (see Roussel, column 12, line 1-9, "processing 128-bit instructions using existing 64-bit hardware systems without significant changes to the hardware) and "a plurality of the M/m-bit data can be processed through the plural steps selected among the four steps at the same time according to a predetermined timing" (see Roussel, Fig. 4A and Fig. 4B, Fig. 4A discloses a plurality of the input data "M" with the width of 128 bits is divided by two of the 64 bits data after ports 1-3. Fig. 4B shows that at same time T, plural steps, to be exact two steps, have been processed. Four steps have been processed at time T+1 etc).

Response to Arguments

11.   On page 15 of the Applicants' Response, the Applicants argue that Yang and/or Roussel, alone or in combination, teach or suggest amended claim 1 of the invention.

12.   For the amended paragraph of claim 1, Lee teaches all the limitation in the claim. Please refer to the 103 rejection to claim 1 above.

13.   The Applicants also argue on page 15 that Yang teaches away from dividing up the input data.

14.   The Examiner rejected "dividing up the input data" in the Non-final Office Action

by Roussel; and the Examiner does not rejecting the limitation that is a teaching of

Yang; therefore, the applicants' argument is moot.

15.   The Applicants also argue on page 16 that Yang teaches away from performing

the transform of key mixer on the first input data while simultaneously performing the

transform of the mixer on a second input data, where the first and second input data is

half the key value of inputted data.

16.   First of all, the claims in the application do not include the limitation that states

above. The best description in the claims that similar to it was in claim 10 "a plurality of

the M/m-bit data can be processed through the plural steps selected among the four

steps at the same time". It was rejected by Yang in view of Roussel. Please refer the

rejection of the specific portion in claim 10 above. This amended limitation to claims 1,

3, 5, 9 and 11 was rejected under 35 U.S. C. 103 (a). Please refer to the rejection to

those claims.

17.   The Applicants also argue the motivation to combine the references of Yang and

Roussel on page 16. The Applicants state "because Yang requires the key value (i.e.

128, 192, or 256) used in rijndael block cipher algorithm, one skilled in the art would not

have been motivated to use the staggering execution of a single packed data instruction

using the same circuit from Roussel where the key values would less that 128, 192, or

256 respectively".

18.   The Examiner respectfully disagrees. Firstly, the claims in the application do not

state "the key values would less than 128, 192, or 526". All the Applicants stated about

the key values were "N-bit input key" in claims 1, 3, 5, and 11. It does not define "N" is

less than 128, 192, 526. The staggering execution of data was known in the art for one

ordinary skilled in the art at the time of the invention; therefore, it is obvious to combine

the teaching from Roussel to Yang to achieve dividing up the input data and process

data simultaneously.   Furthermore, Lee teaches the feature more explicitly. Please

refer to the rejection on claims 1, 3, 5, 9, and 11.

19.   The Applicants also argue that "Yang teaches away from performing different

transforms on the two different inputted data having partial key values before the end of

each round at the same time" on page 16.

        The Examiner respectfully disagrees with Applicant's argument. Firstly, the

limitation is not in claims of application. Secondly, the Examiner rejected "performing

different transforms on the two different inputted having partial key values" by Roussel.

Finally, Lee teaches the limitations explicitly. Please refer to the rejection on claims 1,

3, 5, 9, and 11.Any inquiry concerning this communication or earlier communications

from the Examiner should be directed to JING SIMS whose telephone number is

(571)270-7315. The Examiner can normally be reached on 7:30am-5:00pm EST, Mon-

Thu.

Conclusion

20.   The Applicants amendment necessitated the new ground(s) of rejection

presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See

MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in

37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

9.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jing Sims whose telephone number is (571) 270-7315.

The examiner can be normally reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Thomas Pham can be reached on (572)272-3689. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jing Sims   12/16/2008

/J.S./

/THOMAS K PHAM/
Supervisory Patent Examiner, Art Unit 4148